



Safeguarding Information Assets in Higher Education

The Role of the CSO

By Rodney Petersen

A campus information system becomes unavailable because a hacker has exploited a vulnerability in the operating system and rendered the application unusable. A faculty member's laptop, which contains research data including personally identifiable information on research subjects, turns up missing. A college's homepage is altered, without authorization, to include sexually explicit content. A private organization's Web site is the subject of a computer-generated attack that originates from an Internet connection at a university. Increasingly, crises such as these are referred to the Chief Security Officer (CSO) to help coordinate an institutional response. For higher education, the CSO is an important strategic and intellectual resource in the protection of information assets and the design of future information systems.

Rodney Petersen is Policy Analyst and Security Task Force Coordinator for EDUCAUSE.

The CSO is already a valuable resource in other sectors. The Federal Information Security Management Act (FISMA) mandates that U.S. federal government agencies appoint a CSO. Many state governments have also moved to create an information security function, either due to state legislation or due to legitimate interests to support e-government initiatives and safeguard citizens' information. The private sector too has embraced the CSO function, largely because of compliance requirements and internal business needs.



The label "CSO" is perhaps a little misleading in the context of information security. Although it was initially used to describe the person responsible for IT security, it is also used at some companies to describe "the leader of the 'corporate security' function, which includes the physical security and safety of employees, facilities and assets." This person might also hold the title of Vice President or Director of Corporate Security.¹ Chief Information Security Officer (CISO) is probably a more accurate title for the person responsible for IT security. According to CSO magazine's 2005 "State of the CSO" survey, the three most common titles for the top security executive are (1) CISO (21%), (2) Manager of Security (21%), and (3) Director of Security (20%). The title of CSO was held by 10 percent of the respondents, although this reflected a 2 percent increase since 2004.²

The "State of the CSO" survey also found that CSOs are increasingly reporting to the Chief Information Officer (CIO) or the Chief Technology Officer (CTO): 38 percent in 2005, compared with 29 percent in 2004. This increase reflects a downward trend in the number who report directly to the CEO/president: from 13 percent in 2004 to 7 percent in 2005.³ This trend in reporting relation-

ships also probably accounts for the shift in who is ultimately accountable for an organization's information security function. According to the IDC's "2005 Global Information Security Workforce Study," the CIO is now deemed the person accountable for information security (according to almost 40% of the respondents), followed by the CEO, the CISO, and the CSO. Despite the trends, the IDC concluded that "the information security profession continues to mature" and that "reporting relationships for security executives and their staffs remain in transition."⁴

One interesting byproduct of the shift in authority and accountability is the question of who takes the fall when a security breach occurs. If the CSO or the security group takes the blame for every incident, chances are that the organization has designated the CSO as the one who makes the final call. According to the CSO magazine article "The ABCs of New Security Leadership," the "final call" belongs to the CEO, president, and board of directors. "Security is supposed to educate the business leaders about the threats the organization faces, about the likelihood and consequences of those threats, and about the costs and effectiveness of possible remedies. Then the business leaders can make the decisions on acceptable risk." That is why "risk management" is an increasingly important responsibility of the CSO. Similarly, it might account for why the 2005 "State of the CSO" survey found the title of Chief Risk Officer (CRO) "dropping off the map": zero respondents selected this job title in 2005, compared with 1 percent in 2004.⁵

The responsibilities for the CSO differ based on size and type of organization. More important, the duties reflect the scope of authority of the position. A CSO who is responsible for both physical and logical/digital security might have the following responsibilities as part of the job description, according to CSO magazine:

- Oversee a network of security directors and vendors who safeguard the company's assets, intellectual property and computer systems, as well as the physical safety of employees and visitors.

- Identify protection goals, objectives and metrics consistent with corporate strategic plan.
- Manage the development and implementation of global security policy, standards, guidelines and procedures to ensure ongoing maintenance of security. Physical protection responsibilities will include asset protection, workplace violence prevention, access control systems, video surveillance, and more. Information protection responsibilities will include network security architecture, network access and monitoring policies, employee education and awareness, and more.
- Maintain relationships with local, state and federal law enforcement and other related government agencies.
- Oversee incident response planning as well as the investigation of security breaches, and assist with disciplinary and legal matters associated with such breaches as necessary.
- Work with outside consultants as appropriate for independent security audits.⁶

CSOs come predominantly from an information systems background (63%). Other common backgrounds include corporate security (35%), military (32%), law enforcement (21%), business operations (19%), and audit (18%).⁷ According to CSO magazine, the typical qualifications for a job description might include the following:

- Must be an intelligent, articulate and persuasive leader who can serve as an effective member of the senior management team and who is able to communicate security-related concepts to a broad range of technical and non-technical staff.
- Should have experience with business continuity planning, auditing, and risk management, as well as contract and vendor negotiation.
- Must have strong working knowledge of pertinent law and the law enforcement community.
- Must have a solid understanding of information technology and information security.⁸

The emphasis on communication skills is especially important because executives and decision-makers often perceive that information security is too technical for them to understand. That is why CSO magazine reported that “tech talk and copspeak” are OUT and “business language and communication skills” are IN. “Talking in business terms with executives can . . . be a tremendous asset in advancing the CSO’s agenda. . . . Building and maintaining strong relationships with business executives and their groups requires the CSO to assume a number of different guises: educator, strategist, negotiator, interpreter and, sometimes, disciplinarian.”⁹

The CSO in Higher Education

Despite the precedent for the CSO role in industry and government, the responsibilities for IT security in a typical college or university have taken a very different path. One significant reason is that the corporate model for creating C-level executive positions (e.g., CEO, CFO, CIO) does not reflect a typical campus organizational structure, which is led by presidents, provosts, or other senior administrators of the institution. The differences are magnified when comparing the typically centralized organization of corporations with the often decentralized or distributed nature of a college or university. CIOs, a relatively new phenomenon in higher education, run up against the natural resistance to adding another C-level executive as part of

2003 and 2006.¹⁰ These reports contain some very helpful data regarding IT security in higher education generally and regarding the organization and leadership for IT security more specifically. For example, the results show that since 1994, there has been a steady increase in the establishment of IT security positions at colleges and universities. According to the 2006 study, 34.9 percent of the respondents indicated that their institution had a formally designated individual as its IT security officer (or equivalent), with 55.5 percent having been appointed since 2003. The position of IT security officer is full-time at 32.2 percent of the institutions, up from 20 percent in 2003. However, 70.6 percent of the full-time IT security officers work at doctoral institutions.

The responsibility for IT security primarily resides with the IT security officer or equivalent (34.9%), a 55.8 percent rate of change since 2003. The greatest rate of change (113%) was for CIOs or equivalent (14.3%). Together, the director of networking (21.8%) and other IT management (23.9%) still account for the largest share of responsibility, although responsibilities appear to be shifting quickly away from them (-28.9% rate of change and -22.7% rate of change, respectively).

Of the respondents in the recent ECAR survey, 18 percent indicate that the person in charge of IT security holds one IT security certificate. Additionally, 20.5 percent of the IT security staff had earned one form of certification. The

Another significant change is the movement toward one central IT security unit or function (61.8%), as opposed to spreading responsibility across multiple units (32.7%). In 2003, the approaches were almost identically reversed, with only 38.7% reporting a central IT security unit. Additionally, overall security staffing is on the increase, with 4.7 percent having ten or more employees, 8.1 percent having three employees, 13.2 percent having two employees, and 21.6 percent having one full-time employee. Nonetheless, 38.5 percent still have less than one full-time employee managing security. Less than 1 percent indicated an expected staff decrease; 50.2 percent expected no change; 24.4 percent expected to add one staff member; and 7.7 percent expected to add two or more.

In general, a systematic approach to information security involves attention to *people, process, and technology*. Because the CSO typically resides in the IT organization and usually possesses technology expertise, emphasis tends to be placed on the technological interventions that can help improve computer and network security. At some institutions, an IT Policy Officer or other staff might provide leadership to the people and process strategies and tactics. Some have argued that *people* are the most important part of the equation, including the leadership provided by the CSO. Additionally, responsibility for information security is shared by individuals capable of preventing security incidents, which is why awareness efforts

Because the CSO typically resides in the IT organization and usually possesses technology expertise, emphasis tends to be placed on the technological interventions that can help improve computer and network security.

the campus hierarchy. Finally, unlike the corporate sector, the nonprofit sector is unable to pass along the cost of security to the customer, so the tendency has been to ease into the hiring of security staff, often promoting or reassigning from within the IT organization. Therefore, the evolution of the CSO role has been very difficult to characterize for the higher education sector.

In an effort to provide an overview of information security in higher education, the EDUCAUSE Center for Applied Research (ECAR) has conducted two security surveys, publishing reports in

most common certifications held are the Certified Information Systems Security Professional (CISSP) (20.8%), the Global Information Assurance Certification (GIAC) (6.8%), and the Certified Information Systems Auditor (CISA) (3.2%). The reported salaries for an IT security officer vary from a range of \$30,000–\$49,000 to \$150,000 plus, with an average salary in the \$75,000–\$99,000 range (the average was in the \$50,000–\$74,000 range in 2003). Not unexpectedly, the salaries for IT security officers at doctoral institutions are highest, followed very closely by MA institutions.

and training programs are such important ingredients.¹¹ There has also been much criticism of the incompatibility between academic organizations and the need to develop a “culture of security.” Therefore, the *process* needs are increasingly important for colleges and universities and include such elements as security strategy, policy development and enforcement, physical security, and security program administration. Some examples of the roles and responsibilities that a typical CSO or his/her staff in higher education might fulfill in the areas of *technology, people, and process* include the following:

- Develop, implement, and maintain a written “information security program” that addresses people, process, and technology and contains administrative, technical, and physical safeguards¹²
- Develop and deliver security-awareness presentations for students, faculty, and staff
- Conduct or arrange for training sessions for IT staff or individuals responsible for safeguarding data
- Perform periodic risk assessments that identify and locate information assets and assess vulnerabilities
- Conduct a risk analysis that identifies mitigation techniques and resource needs
- Develop and periodically update information security policies and procedures that address areas such as individual employee responsibilities for information security practices
- Implement security technologies designed to prevent, detect, and deter security incidents
- Coordinate with other IT staff in the areas of user identification and authentication, user account management, user privileges, configuration management, event and activity logging and monitoring, and other technical best practices¹³
- Coordinate with appropriate process owners for business continuity planning and disaster recovery
- Work with “data stewards” (officials responsible for different types of
- Work closely with internal IT application developers to create quality-assurance processes that address security across the software development life-cycle
- Develop metrics for measuring success and regularly report to management and the governing board on progress and challenges
- Collaborate with other colleges and universities to share information or resources, as necessary, to improve the overall security of the higher education sector

Key Elements for Success

Higher education institutions face issues of risk, liability, business continuity, costs, and national repercussions as they increasingly move their core activities to the Internet. Colleges and universities also play a unique role as the managers of some of the largest collections of computers on many of the fastest networks. The stakes are high, and the need to exercise energy and resources effectively is paramount.

The first key element for success is building a program around a solid system of information security governance (ISG). To help institutions determine the degree to which they have implemented an ISG framework at the strategic level, the EDUCAUSE/Internet2 Computer and Network Security Task Force has produced the “Information Security Governance Assessment Tool for Higher Education.”

create the structure that can help lead to the allocation of necessary and appropriate resources.

The second key element for success is the development, implementation, and periodic review of a comprehensive IT security plan. According to the 2006 ECAR security study, only 11.2 percent of institutions reported that such a plan was in place; 20.4 percent reported that no IT security plan of any type was in place at their institution. The remaining respondents (66.6%) reported that they had a partial plan in place. According to the survey results, respondents at institutions with IT security plans in place characterize their IT security programs as more successful and note that they feel more secure today. Planning also increases responsiveness to government regulation and metrics.¹⁵ Many CSOs report that they spend too much time responding to incidents and getting drawn into day-to-day operational matters. Planning should be a priority in a CSO’s job duties and in the allocation of his or her time.

The final key element for success is the establishment of appropriate benchmarks and metrics that will allow the CSO to chart progress and to demonstrate value to stakeholders. This is not easy. The “Report of the Best Practices and Metrics Team,” prepared by the Corporate Information Security Working Group (on which EDUCAUSE participated), outlines some “Information Security Program Elements and

The final key element for success is the establishment of appropriate benchmarks and metrics that will allow the CSO to chart progress and to demonstrate value to stakeholders.

institutional data—human resources, registrar, etc.) to establish appropriate safeguards

- Coordinate plans and protocols for emergency incident response
- Establish a cooperative working relationship with law enforcement—including campus police or public safety and local, state, and federal officials—for reporting incidents and conducting investigations
- Establish security requirements for vendors of commercial software and devise contract language to place responsibility for security on the application provider

This tool is not intended to provide a complete and detailed list of information security policies or practices that must be followed. Rather, it is intended to help a president or other institutional leaders identify general areas of concern related to the ISG framework. Not surprisingly, according to the 2006 ECAR security study, the biggest barrier to IT security is lack of resources (64.4%), especially at smaller institutions. Similarly, respondents who believe their institution provides necessary resources give higher ratings for IT security program success and for their current sense of IT security.¹⁴ Institutions with a strong ISG framework

Supporting Metrics.” It further breaks down the responsibilities for boards of directors/trustees, for management, and for technical staff. The report restates a popular dictum: “What gets measured gets done.” Urging the board, management, and technical staff to identify, approve, and articulate the set of metrics supporting the information security program, the report notes: “Metrics report how well policies, processes, and controls are functioning, and whether or not desired performance outcomes are being achieved.”¹⁶ Several years ago, Jeffrey Schiller, MIT network manager, put it this way: “Security is a negative

Information Security Governance Assessment Tool for Higher Education: People

A successful information security program depends on the effective implementation of information security governance. The EDUCAUSE/Internet2 Computer and Network Security Task Force has developed the “Information Security Governance Assessment Tool for Higher Education” to help colleges and universities determine the degree to which they have implemented an information security governance framework at the strategic level within their institution. The following set of questions—from Section III: People—assesses the organizational aspects of an information security program.

- Is there a person or organization that has information security as their primary duty, with responsibility for maintaining the security program and ensuring compliance?
- Do the leaders and staff of your information security organization have the necessary experience and qualifications?
- Does your information security function have the authority it needs to manage and ensure compliance with the information security program?
- Does your information security function have the resources it needs to manage and ensure compliance with the information security program?
- Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?
- Has specific responsibility been assigned for the execution of business continuity and disaster recovery plans (either within or outside the information security function)?
- Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function?
- Is someone in the information security function responsible for liaising with units to identify any new security requirements based on changes to operations?
- Does the information security function actively engage with other units (human resources, student affairs, legal counsel) to develop and enforce compliance with information security policies and practices?
- Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies?
- Are the senior officers of the institution ultimately responsible and accountable for the information security program, including approval of information security policies?
- Do the unit heads and senior managers have specific programs in place to comply with information security policies and standards with the goal of ensuring the security of the information and systems that support the operations and assets under their control?
- Have you implemented an information security education and awareness program such that all administrators, faculty, staff, contractors, external providers, students, guests, and others know the information security policies that apply to them and understand their responsibilities?

Completing the tool (which also includes sections on Organizational Reliance on IT, Risk Management, Processes, and Technology) results in an *overall security evaluation rating*. The tool is available at <<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>>.

deliverable. You don't know when you have it. You only know when you've lost it."¹⁷ It is up to the CSO to consistently demonstrate the value of the information security program and to demonstrate how the deliverables are contributing to the broader institutional goals.

Conclusion

There are significant differences in how a small versus a large college or university

might approach the organization of an information security program and the assignment of leadership. There are also significant differences in approach for government, for private industry, and for academia. One size does not fit all. However, there are lessons to be learned across sectors, regardless of size and type. The common goal in all cases is to protect the organizational information assets and to contribute to the security of interdepen-

dent critical infrastructures. Given the importance of the charge and the amount of work to be done, colleges and universities must empower an individual, such as the Chief Security Officer, or a team with the authority, the resources, and the support needed to effectively maintain an information security program. *e*

Notes

1. "What Is a Chief Security Officer?" CSO, December 1, 2005, <http://www.csoonline.com/research/leadership/cso_role.html>.
2. Julie Hanson, "The State of the CSO—Part 1," CSO, June 1, 2005, <http://www.csoonline.com/cso_research/report89.html>.
3. Ibid.
4. Allen Carey, "2005 Global Information Security Workforce Study," *IDC White Paper*, December 2005, <http://www.securitymanagement.com/library/globalinformation_itsecurity0206.pdf>.
5. "The ABCs of New Security Leadership," CSO, February 17, 2004, <http://www.csoonline.com/fundamentals/abc_leadership.html>; Hanson, "State of the CSO."
6. "What Is a Chief Security Officer?"
7. Hanson, "State of the CSO."
8. "What Is a Chief Security Officer?"
9. "The ABCs of New Security Leadership."
10. Robert B. Kvavik and John Voloudakis, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," *EDUCAUSE Center for Applied Research (ECAR) Study*, vol. 5 (2003), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERSO305>>; Robert B. Kvavik with John Voloudakis, "Safeguarding the Tower: IT Security in Higher Education, 2006," *EDUCAUSE Center for Applied Research (ECAR) Study*, forthcoming, fall 2006. In addition, the annual EDUCAUSE Core Data Service (<http://www.educause.edu/coredata>) provides some useful data for institutions that desire to benchmark their organization and services against institutions of similar size and type.
11. See the statement by Freeman Hrabowski, President of the University of Maryland–Baltimore County (UMBC), who said that "human error" was responsible for an unauthorized disclosure of Social Security numbers at his institution: "Cyber Security on Campus," Executive Awareness Video, <<http://www.educause.edu/LibraryDetailPage/666?ID=CSD4121>>.
12. Required for compliance with the Gramm-Leach-Bliley Act; see "Standards for Safeguarding Customer Information: Final Rule," Federal Trade Commission, 16 C.F.R. Part 314.
13. For a complete listing of technical best practices and metrics, see Corporate Information Security Working Group, "Report of the Best Practices and Metrics Teams" (U.S. House of Representatives, Government Reform Committee, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, November 17, 2004), <<http://www.educause.edu/LibraryDetailPage/666?ID=CSD3661>>.
14. Kvavik and Voloudakis, "Safeguarding the Tower."
15. Ibid.
16. Corporate Information Security Working Group, "Report of the Best Practices and Metrics Teams."
17. "Security on Campus: An Interview with Jeffrey I. Schiller," *Syllabus*, August 1, 2002, <<http://www.campus-technology.com/article.asp?id=6586>>.